TRICARE

TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Documentation of Security Actions

HIPAA Security • November 2003

Standard Requirement

The Security Rule requires covered entities to "maintain the policies and procedures implemented to comply with the [Security Rule] in written (which may be electronic) form" and maintain a "written (which may be electronic) record" of any "action, activity or assessment" that is required by the standards and implementation specifications of the Rule.

This standard includes two parts. The first part requires covered entities to document in written format (paper or electronic) policies and procedures pertaining to the protection of electronic protected health information. When organizations develop and maintain their policies and procedures as part of an "oral tradition" only, they become vulnerable to several threats. Orally developed and transmitted policies tend to drift in response to local circumstances thus helping produce varying practice across the organization. In the absence of written rules, organizations inconsistently and incompletely train personnel and find consistent enforcement difficult or impossible. Maintaining policies and procedures in written format safeguards against these threats. The second part requires covered entities to document the results of implementing the policies and procedures when required by a standard or implementation specification. That would include risk analyses and risk management reports conducted as part of the security management process, security incident reports, all business associate contracts, designations of security officers, and so on. This serves several purposes. Examination of the records for patterns of activity can reveal threats and vulnerabilities, allowing the covered entity to take action to improve the security of protected health information. Because written records demonstrate compliance with policies and procedures, auditors and other surveyors often request to review them during inspections. And finally written records can demonstrate due diligence. Documentation must be "detailed enough to communicate the security measures taken and to facilitate [the] periodic evaluations" required by the security evaluation standard of the administrative safeguards. (Final Rule, p.8361)

Implementation specifications

There are three required implementation specifications associated with the documentation standard:

- Time limit
- Availability
- Updates

TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Documentation of Security Actions

HIPAA Security • November 2003

The first implementation specification, time limit, calls for each covered entity to keep all policies and procedures required by the HIPAA security rule until six years after they are no longer in effect. They must also keep the documented results of actions, activities, assessments, or designations created as a result of the HIPAA security rule for six years. This ensures that the information is available if needed to answer legal questions and other inquiries that might arise.

The second implementation specification, availability, requires covered entities to make their security documentation available to those who need it. In keeping with the flexible nature of the HIPAA Security Rule, this mandatory implementation specification does not dictate how the covered entity should provide documentation to those who need it. It allows the covered entity to choose methods and intervals that are appropriate to its environment and business structure. Those people with specific security responsibility and users must have access to the written policies and procedures. Ready access to the written procedures improves the likelihood staff members will follow them. Covered entities can accomplish this in several ways including, providing offices or individual employees with copies of policy documents and standard operating procedure manuals, training manuals, and web pages.

The third implementation specification, updates, makes covered entities responsible for keeping the documentation current by reviewing it "periodically," and updating it as needed, "in response to environmental or operational changes affecting the security of the electronic protected health information." Changes in the way we do business, upgrades and new equipment and software, new laws and regulations, and a constantly changing threat environment can require changes to policy and operating procedures. Out of date documentation poses a risk to the systems and the information they store and process. A periodic review of those policies and procedures helps to ensure that they are always accurate and appropriate. In keeping with the principle of scalability, there is no fixed standard for this — "the need for review and update will vary dependent on a given entity's size, configuration, environment, operational changes, and the security measures implemented." (Final Rule, p.8361)

See also:
45 CFR 164.316(b)